Tietosuoja-asetus verkkokaupalle - Muistilista onnistuneeseen implementointiin

Valtteri Sivula

2020 Laurea

Laurea-ammattikorkeakoulu

Tietosuoja-asetus verkkokaupalle - Muistilista onnistuneeseen implementointiin

Valtteri Sivula
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Toukokuu, 2020

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutusohjelma
Tradenomi (AMK)

Valtteri Sivula

Tietosuoja-asetus verkkokaupalle - Muistilista onnistuneeseen implementointiin

Vuosi 2020 Sivumäärä 36

Opinnäytetyön tavoitteena oli tutkia aloittavan verkkokaupan vastuita ja velvollisuuksia EU:n yleisen tietosuoja-asetuksen näkökulmasta. Tarkoitus oli tuottaa näiden tutkimusten perusteella helposti lähestyttävä tärkeimpien asioiden muistilista, mitä seuraamalla aloittava verkkokauppa osaa ymmärtää omat vastuut ja velvollisuudet, sekä asettaa omat toimenpiteet riskejä vastaavaan kontekstiin heti toimintoja aloittaessa.

Opinnäytetyön toteutusmenetelmä oli tutkimuksellinen kehitystyö. Tutkimusmenetelmän avulla oli tarkoitus tuottaa aineistotutkimuksien perusteella kehitystoimintaa tutkimuskysymyksen ympärille, sekä tuottaa ratkaisu konkreettiseen ongelmaan verkkokaupan tietosuoja-asetuksen vaatimusten, velvollisuuksien ja toimenpiteiden ymmärtämisestä verkkokauppaa perustettaessa. Työn teoreettisella osuudella oli tarkoitus asettaa yllä mainitut seikat tarpeelliseen kontekstiin ja osaksi isompaa kokonaisuutta.

Tutkimuksen tuloksena selveni verkkokaupan vastuiden koostuminen monesta erillisestä osiosta, jotka kaikki yhdessä muodostavat hyvän dokumentaation kanssa osoitusvelvollisuuden onnistumisen. Näiden perusteella yrityksen tarpeisiin luotiin tiivistetty muistilista, jonka avulla verkkokauppa pääsee heti toimintoja aloitettaessa selville tietosuoja-asetuksen tärkeimmistä velvollisuuksista ja toimenpiteistä.

Asiasanat: Tietosuoja-asetus, GDPR, Verkkokauppa

Laurea University of Applied Sciences
Degree Programme in Business Infromation technology
Bachelor's Thesis

Valtteri Sivula

Abstract

Implementation of GDPR - Important Steps for an Online Startup Company

Year 2020 Pages 36

The objective of this Bachelor's thesis was to study responsibilities and duties set by general data protection regulation (GDPR) from a point of view of online startup company. The purpose was to produce an easily approachable set of instructions from which the startup can follow few easy steps to ensure concept of GDPR and understand its responsibilities and duties as an entrepreneur. This set of instructions was made for private entrepreneur who will operate small online store in the future.

The research method of this thesis was material research and development. Material research was used to generate concrete development ideas from source material and to give GDPR some background and context. Research question what needs to be addressed and comprehended from GDPR as online store builds up operations was leading the development part of thesis.

The results of this thesis was that good GDPR practice consists of several different tasks and observations, which all together with successful documentation, makes responsibilities clear from the very start. From these tasks and observations a simple step-by-step guide was built to help startup the basic needs for a successful implementation of GDPR.

Keywords: General Data Protection Regulation, GDPR, Online store

Sisällys

1 Johdanto

Tämän opinnäytetyön ensisijaisena tavoitteena on toimittaa asiakasyritykselle lainsäädäntöön, sekä hyviin tietosuojatapoihin pohjautuva, tärkeimpien asioiden muistilista EU:n yleisen tietosuoja-asetuksen (GDPR) onnistuneeseen implementointiin. Työn tietoperustan tarkoituksena on auttaa asiakasyritystä asettamaan tietosuoja-asetuksen velvoittamat toimenpiteet oikeisiin mittasuhteisiin ja osaksi isompaa kontekstia. Lisäksi työ toimii osana asiakasyrityksen tarvetta selventää omia vastuita ja velvollisuuksia, toimintaa rekisterinpitäjän ominaisuudessa sekä varmistaa osaltaan asiakasyrityksen osoitusvelvollisuuden täyttyminen.

Yrityksen avuksi on rakennettu erillisenä liitteenä löytyvä lyhyt muistilista yllä mainittujen asioiden huomioimiseksi. Nämä muistilistassa mainitut osiot perustellaan, ja osin ohjeistetaan, tarkemmin työn konkreettisessa osiossa. Vaikka työn konkreettisesta osuudesta löytyy muutamia toimintamalleja, on työn pääpaino kuitenkin ollut mitä tehdä -listauksessa, ei niinkään miten tehdä. Muistilistasta nousevien toimenpiteiden suoritustapa jätetään suurilta osin yrityksen omaan harkintaan.

Asiakasyrityksenä opinnäytetyössä on toimintojaan aloittava verkkokauppa. Verkkokauppa on tehnyt markkinatutkimuksen, liiketoimintasuunnitelman ja kilpailuttanut verkkokauppa-alustan järjestäjän, mutta ei ole vielä ajanut toimintojaan ylös. Markkinaympäristö keväällä 2020 muuttui nopeasti koronaviruksen leviämisen johdosta, ja vaikka tämä saattaisikin jossain määrin tukea verkkokauppaa, on yleinen tilanne kuitenkin niin epävarma, että kaikki toiminta on jätetty odottamaan tilanteen selviämistä. Verkkokaupan toimintaympäristö tulee olemaan vähittäiskauppa verkon välityksellä, eli kivijalkatoimintaa ei löydy. Asiakasyrityksen pyytämän anonymiteetin sekä yrityksen epävarman tilanteen takia tässä opinnäytetyössä yritykseen viitataan nimellä verkkokauppa tai asiakasyritys.

Tätä opinnäytetyötä tullaan käyttämään asiakasyrityksessä yhtenä osana liiketoimintamallin velvoittavien tietosuoja-asetusten vastuiden ja velvollisuuksien määrittelyssä. Tärkeimpänä onnistumisen kriteerinä voidaan siis pitää onnistunutta tietosuoja-asetuksen käyttöönotto, sen jatkuvaa seurantaa sekä ymmärrystä omista velvoitteista, vastuista ja dokumentaation tärkeydestä. Tarkoituksena on, että osoitusvelvollisuuden määrittämät velvollisuudet osataan ottaa huomioon jo heti toimintoja aloitettaessa. Osiltaan määrittelyt ja kaikki tarvittavat sopimukset tehdään verkkokaupan palveluntarjoajan sekä muiden henkilötietojen käsittelijöiden kanssa. Tämä työ antaa muistilistan tietosuoja-asetuksen implementointiin sekä auttaa ymmärtämään kontekstin teoriaosuuden kautta.

2 Työn lähtökohdat

Tämä opinnäytetyö lähtee selvittämään aloittavan verkkokaupan tietosuoja-asetuksen velvollisuuksista kumpuaviin toimenpiteisiin, sekä vastuiden ja velvollisuuksien määrittelyyn. Nämä toimenpiteet ja määrittelyt löytyvät hajautettuna eri lähteistä, ja varsinkin aloittavan yrityksen on haastavaa poimia useasta tietolähteestä tärkeimmät ja juuri itselle relevantit tiedot. Työn lähtökohtana on vastata perustellusti seuraaviin tutkimuskysymyksiin: Mitä kaikkea tietosuoja-asetuksessa on otettava huomioon toimintoja aloitettaessa? Mitä osoitusvelvollisuus vaatii aloittavalta yritykseltä?

2.1 Työn kehittämistavoitteet

Työn tarkoituksena on tuottaa yhdelle dokumentille askelmerkit mitä seuraamalla edellä mainitut asiat tulevat otetuksi huomioon. Nämä askelmerkit rakennetaan valmistamalla yksinkertainen muistilista, mistä selviää kaikki tärkeimmät aloittavan yrityksen tietosuoja-asetuksen velvoitteet. Tämä liitteenä löytyvä, verkkokaupalle toimitettava muistilista, on tarkoitus tiivistää mahdollisimman lyhyeksi, mutta työn käytännön osuus on rakennettu tukemaan tätä tiivistettyä listaa antamalla tarkempia kuvauksia ja esimerkkejä toimintamalleista. Työ ei ole täysi läpileikkaus tietosuoja-asetuksesta, vaan sen pääpainona on huomioida aloituksessa huomioitavat asiat, sekä tuoda tietosuoja-asetusta esille helposti ymmärrettävään muotoon, mikä osaltaan auttaa huomioimaan tietosuojan myös tulevaisuudessa.

Lisäksi katsauksella tietosuoja-asetukseen yleisesti on tarkoitus asettaa konteksti mitä vasten aloittavan verkkokaupan on mahdollista peilata omia toimintojaan. Yritys käyttää tätä työtä yhtenä osana toimintojen, velvollisuuksien, vastuiden ja oikeuksien määrittelyä yhdessä muiden dokumenttien, kolmansien osapuolien ja muiden ohjeistusten ja sopimuksien kanssa. Lisäksi työssä huomioidaan yhteistyö henkilötietojen käsittelijän kanssa ja pureudutaan tarkemmin vastuiden määrittelyyn ja verkkokaupan osoitusvelvollisuuden onnistumiseen.

2.2 Aihealueen rajaus

Tietosuoja-asetus ja sen implementointi on laaja alue, ja sen toimeenpano on jossain määrin riippuvainen mm. yrityksen koosta, toimialasta, toimintaympäristöstä. Tämä opinnäytetyö keskittyy vain asiakasyrityksen toimintojen varmistamiseen, eikä se välttämättä toimi oppaana suoraan muille yrityksille. Opinnäytetyön teoreettinen viitekehys sekä vastuupyramidi skaalauntuvat tosin myös suurempiin yrityksiin, mutta toimintamallit riippuvat lähtökohtaisesti eri tilanteista. Työn tarkoituksena ei ole antaa juridisia ohjeita, vaan se toimii vain toimintamallina asiakasyritykselle. Työstä on jätetty pois myös yleiset tietoturvavaatimukset aina työskentelytavoista, sähköpostikäytännöistä ohjelmistovaatimuksiin ja perehdytään vain tietosuoja-asetuksen asettamiin tärkeimpiin velvoituksiin.

Verkkokauppa voi kerätä tilausten toimittamista varten erilaisia tietoja, esimerkiksi nimi, osoite, puhelinnumero, tilauksen summa ja tilatut tuotteet. Lisäksi verkkokauppa saattaa tulevaisuudessa päätyä keräämään asiakaspohjasta muutakin tietoa mitä tässä työssä ei ole otettu huomioon. Työ ei ota kantaa siihen mitä henkilötietoja, tai mihin käyttötarkoitukseen asiakasyrityksen kannattaa rekistereitä kerätä, se jää asiakasyrityksen omaan harkintaan. Työ osoittaa vain toimintaperusteet ja vastuut rekistereiden keräykselle.

ePrivacy on EU:n komission käsittelyssä oleva asetus sähköisen viestinnän tietosuojasta, joka tulee täydentämään EU:n yleistä tietosuoja-asetusta ilmestyessään. ePricacyn tärkeimpänä sisältönä tulee olemaan henkilötietojen tunnistamiseen liittyvät kokonaisuudet, profiloinnit ja viestinnän kohdentaminen. (Pyhtiä 2019, 38). Euroopan unionin komission mukaan tarkoituksena on suojata sähköisen viestinnän yksityisyyden suojaa ja lisätä luottamusta sähköiseen viestintään. ePrivacyn odotetaan muuttavan käytäntöjä ainakin sähköisen suoramarkkinoinnin ja mainosten kohdentamisen kanssa. Alun perin ePrivacyn aikatauluna oli ilmestyä samaan aikaan yleisen tietosuoja-asetuksen kanssa, mutta aikataulu on sittemmin pitkittynyt monta kertaa. Tällä hetkellä, keväällä 2020, ePrivacyn tarkka sisältö ja voimaanastumisen aikataulu on toistaiseksi hämärän peitossa, mutta on mahdollista että asiasisältö tulee muuttumaan tulevaisuudessa asetuksen myötä.

2.3 Keskeiset käsitteet ja lyhenteet

Opinnäytetyössä viitataan useasti seuraaviin käsitteisiin ja lyhenteisiin;

Henkilötieto

Henkilötietona pidetään kaikkia sellaisia tietoja mistä voidaan suoraan tai välillisesti, esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen, tunnistaa tai erottaa yksityinen henkilö. Esimerkkejä henkilötiedoista ovat: Nimi, kotiosoite, sähköpostiosoite, puhelinnumero, henkilökortin numero, auton rekisterinumero, paikannustiedot, IP-osoite, potilastiedot, lemmikin eläinlääkäritiedot tai isoisoisovanhempien perinnöllisiä sairauksia koskevat tiedot (Tietosuojavaltuutetun toimisto 2019a).

Henkilötietojen käsittely

Henkilötietojen käsittelyllä tarkoitetaan esimerkiksi henkilötietojen keräämistä, säilyttämistä, käyttöä, siirtämistä tai luovuttamista. (Tietosuojavaltuutetun toimisto 2019a.)

Henkilötietorekisteri

Mikä tahansa tietojoukko mikä pitää sisällään jäsenneltyjä henkilötietoja. Teknisesti henkilötietorekisteri voi olla sähköisessä muodossa esimerkiksi ohjelmisto, Excel -tiedosto tai fyysisessä muodossa, esimerkiksi paperinen rekisteri.

Rekisteröity

Luonnollinen henkilö jonka tietoja on tallennettu rekisteriin.

Sopimukseen perustuva käsittely

Henkilötietojen käsittely sopimukseen perustuen, esimerkiksi asiakas tilaa verkkokaupasta tuotteita.

Suostumukseen perustuva käsittely

Henkilötietoja käsitellään kuluttajan antaman luvan perusteella, esimerkiksi lupa sähköpostin käyttämisestä suoramarkkinointiin.

Opt-in / Opt-out

Opt-in on prosessi missä kuluttaja tekee aktiivisen hyväksynnän toimenpiteisiin esimerkiksi checkboxia klikkaamalla.

Opt-out on prosessi missä kuluttaja tekee päätöksen poistua palvelun piiristä.

GDPR

General Data Protection Regulation. EU:n yleinen tietosuoja-asetus.

LGPD

Lei Geral de Proteção de Dados. Brasilialainen lähestymistapa yleiseen tietosuoja-asetukseen mikä on monilta osin samankaltainen GDPR:n kanssa.

DPIA

Data Protection Impact Assassment. Tietosuojaa koskeva vaikutustenarvionti. Tulee tehdä jos henkilötietojen käsittelyssä huomataan korkeita riskitasoja.

DPO

Organisaatiossa tietosuojasta vastaava taho. Suomessa tietosuojavastaava.

3 EU:n yleinen tietosuoja-asetus

GDPR (General Data Protection Regulation) eli EU:n yleinen tietosuoja-asetus, on Euroopan unionin jäsenmaita koskeva lainsäädäntö millä on yritetty sekä yhtenäistää että suojata henkilötietojen käsittelyä yritysten ja muiden toimijoiden toimesta. Asetus takaa yksityiselle kuluttajalle aiempaa laajemmat oikeudet selvityksiin henkilötietojen tallentamisen osalta. Yksityiselle kuluttajalle tietosuoja-asetuksen käyttöönotto antoi mahdollisuuden selvittää mitä henkilötietoja rekistereihin on tallennettu kunkin toimijan osalta, miksi niitä kerätään, mihin niitä käytetään, ketä varten niitä tallennetaan ja tarvittaessa mahdollisuuden pyytä tietojensa tarkistamista, väärien tietojen muuttamista tai kokonaan tietojensa poistoa. Kuluttajien on päästävä tietoiseksi jo ennen tietojen keräämistä mitä tietoja tullaan keräämään ja mihin niitä käytetään. Tämä yksityisen kuluttajan oikeus velvoittaa rekisterinpitäjät pitämään henkilötiedot tallessa, salattuna, käytettävissä ja valvoa että kuluttajien oikeudet toteutuvat. (Tietosuojavaltuutetun toimisto 2019b.) Yrityksen näkökulmasta tämä tarkoittaa erikseen määriteltyjä vastuualueita, työtapoja sekä osoitusvelvollisuuden toteutumista.

Tietosuoja-asetus velvoittaa kaikkien henkilötietojen tallentamisessa Euroopan unionin alueella, sekä myös Euroopan unionin ulkopuolisten tahojen tietojen tallennusta niiltä osin kun ne tallentavat Euroopan unionin jäsenmaiden asukkaiden tietoja Euroopan ulkopuolelle. Tietosuoja-asetus on annettu keväällä 2016 ja se on otettu käyttöön kahden vuoden siirtymäajalla 25.5.2018 mennessä. Asetus korvasi suoraan aiemman 1995 annetun tietosuojadirektiivin 95/46/EY. (Eur-Lex 2018.)

3.1 Yleisen tietosuoja-asetuksen tarpeet

Jatkuvassa kasvussa oleva verkon kautta tehtävä asiointi on nostanut uudenlaista huolta ihmisten yksityisyydestä ja toimintaympäristön turvallisuudesta. Varsinaisen verkkokaupan lisäksi henkilötietoja käsittelevät erilaiset julkiset toimijat, esimerkiksi terveydenhuolto, sosiaalihuolto, turvallisuuspalvelut tai vaikka hautausurakointi. Myös yritykset tallentavat tietoa omista työntekijöistään. Erilaisten tietosuojalainsäädäntöjen perimmäisenä tarkoituksena onkin suojata sekä yksityistä kuluttajaa että yritystä, tai muuta rekisterinpitäjää, rikolliselta toiminnalta asettamalla rekisterinpitäjälle erinäisiä velvollisuuksia ja kuluttajalle tiettyjä oikeuksia. Kuluttajan yksityisyydensuojan voidaan ajatella muodostuvan sekä yksilön oikeuksista tietää ja vaikuttaa omien henkilötietojen käsittelyyn että rekisterinpitäjien henkilötietojen käsittelyyn liittyvistä velvollisuuksista. (Salminen 2009, 15.)

Tietosuoja digitaalisessa toimintaympäristössä nivoutuu yhteen yleisen tietosuojan kanssa eikä toimi erillään "reaalimaailmasta", samoin kuin tietoverkkorikollisuus - kyberrikollisuus - sulautuu yhteen perinteiseen rikollisuuteen. Rikoksien rajat perinteisen ja kyberrikollisuuden parissa hämärtyvät ja tietoverkkoja käytetään osana omaisuusrikoksia, pankkiryöstöjä, autoon

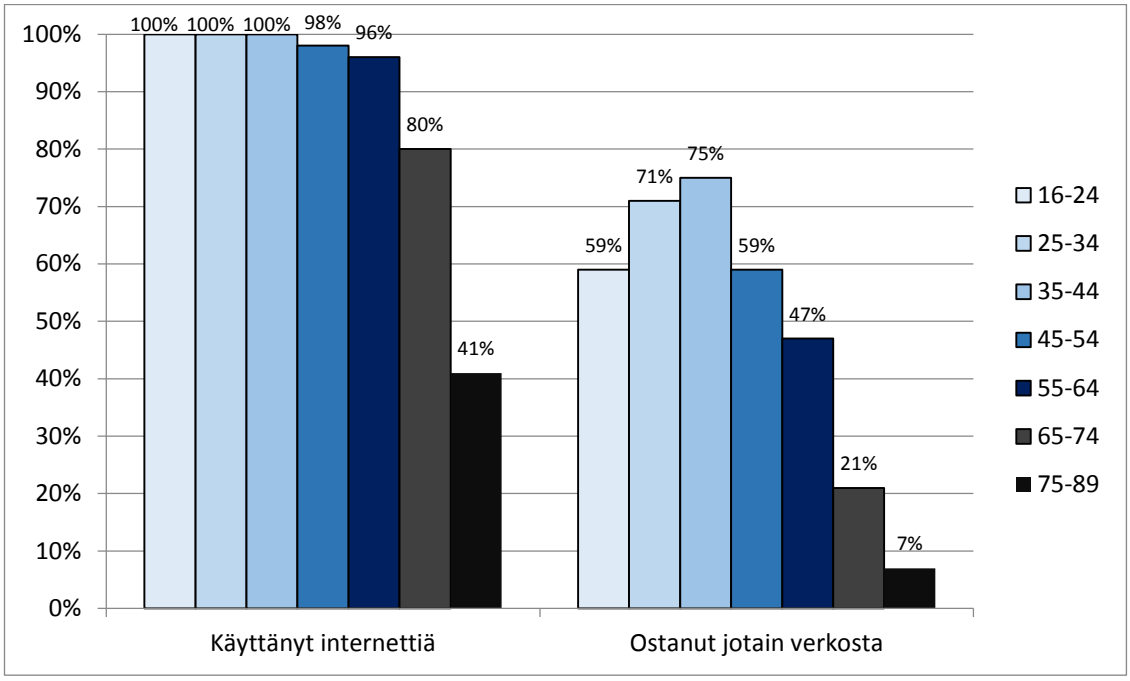
murtautumisia tai mihin vain nähdään mahdollisuus, sillä muuntautuminen digitaaliseen maailmaan on ollut myös nykyaikaisille rikollisille elinehto. (Järvinen & Rousku 2017, 8.)

Tietosuojasta löytyy monta eri tasoa, joiden perimmäisenä tarkoituksena on aina kuluttajan suojeleminen rikoksilta. Verkkorikollisuudessa uhkat voivat tarkoittaa esimerkiksi identiteetin varastamista, päätelaitteeseen kohdistuvaa haittaa, erilaista häiriötoimintaa tai häirintää rahan käsittelyssä tai rahanarvoisen, salatun tiedon löytämistä ja hyödyntämistä.

Uutena huolenaiheena digitaalisessa tietosuojassa on vauhdilla tuleva IoT. IoT, eli esineiden internet, on teollinen internet mistä on povattu seuraavaa suurta tietoteknistä vallankumousta. IoT:llä tarkoitetaan kaikkien tiivistettynä teknisten laitteiden suorittamaa tiedonsiirtoa ja etäohjausta, mitä voidaan suorittaa tietoverkkojen välityksellä. IoT:n tuottama arvonlisäys tulee tietomäärän käsittelystä ja tiedon keräyksestä. IoT on herättänyt laajasti huolto sen osalta, että näiden laitteiden tietoturva ei ole vielä samalla tasolla kuin muiden internetverkkoon liitettyjen laitteiden (Järvinen & Rousku 2017, 6).

Erilaisista huolestuneista puheenvuoroista huolimatta on verkossa tapahtuvan vähittäiskaupan kasvu ollut tasaisessa nousussa pitkin 2010 -luvun. Tietojärjestelmien, kaupan ja kuluttajien astuessa yhä kasvavan globalisaatioon mukaan, on tämä tarjonnut aivan uudenlaisen markkinatilanteen vähittäismyynnille. Entisen kylän, kunnan tai kaupungin potentiaalinen asiakaskunta on vaihtunut parhaimmillaan koko maailman laajuiseen asiakaskuntaan, ja tähän asiakaskuntaan voidaan saada keskenään kommunikoiva yhteys vain dataliikenteen ja näyttöpäätteen yhdistelmällä. Globalisaatio on ilmiönä monimuotoinen, vaikeasti käsitettävä ja tuo mukanaan myös monia ongelmia, mutta markkinatalouden voimat ovat vaikeasti pysäytettävissä, eivätkä jatkuvasti voimistuvat globalisaation vastaiset kriittiset puheenvuorot ole toistaiseksi saaneet suurta ihmismassaa taakseen. Aika näyttää mihin suuntaan kehitys etenee.

Suomella on pitkä ja ansioitunut historia korkean teknologian länsimaana, eikä tätä tietoa vasten ole yllätys, että maan verkkokaupankäynti on maailman mittakaavassa aktiivista. Tilastokeskuksen julkaiseman tutkimuksen mukaan suomalaisista 79 % käyttää internetiä useasti päivässä ja yli puolet 16–89-vuotiaista suomalaisista (50 %) oli ostanut netistä jotain viimeisen kuukauden aikana. (Tilastokeskus 2019.) Kuvio 1 osoittaa aktiivisuuden verkossa sekä verkkokaupassa asioinnin viimeisen kuukauden osalta eri ikäryhmien osalta.



Kuvio 1. Väestön viestintä- ja tietotekniikan käyttö 2019 (Tilastokeskus 2019.)

Huomattavaa on, että kuluttava ikäluokka alkaa olla suurimmalta osin myös verkkokauppaa hyödyntävä ikäluokka. Verkkokaupan tulevaisuus näyttää eittämättä hyvältä, sillä nuoremmat ikäluokat ovat odotetun aktiivisia verkossa, ja odotettavissa on saman aktiivisuuden siirtymistä verkkokauppaan kun he siirtyvät enemmän kuluttavaksi ikäryhmäksi, eli käytännössä työelämään. Vaikka tietosuoja ja yksilön henkilötietojen käsittely aiheuttaa varsinkin osassa kuluttajissa huolta, osin ihan syystä, voidaan varmuudella sanoa että verkkokauppa ei tule vähenemään tulevaisuudessakaan. Tarve tietosuojan jatkuvalle kehitykselle muuttavassa tietojärjestelmäympäristössä on siis erittäin perusteltua.

Euroopan unionin eri jäsenmailla on ollut erilainen lähestymistapa tietosuojaan verkossa. Euroopan unionin tasolla onkin nähty tarve ottaa rooli yleisen tietosuoja-asetuksen myötä yksityisen kuluttajan suojelemiseksi nopeasti muuttuvassa toimintaympäristössä. Toisaalta asetus suojaa myös yrityksiä siinä missä yksityisiäkin, sillä selkeiden vastuiden ja velvollisuuksien määrittäminen helpottaa yritysten työtä sekä selkeyttää esimerkiksi vastuiden jakamista ja mahdollisia ulkoistustoimenpiteitä. Arviossa tietosuoja-asetuksen hyvistä kerrannaisvaikutuksista on otettu huomioon myös ihmisten suurempi luotto verkossa tapahtuvaan asiointiin ja ostoksiin, mutta on jokseenkin epäselvää onko mitään keskimääräistä luoton nousua tapahtunut, sillä mitään yksiselitteistä tutkimustietoa asiasta on vaikea löytää.

Osaltaan tietosuoja-asetuksen tausta-ajatuksena on Euroopan unionin vahva kannanotto yksityisen kuluttajan itsemääräämisoikeuteen, jota voidaan pitää suorana jatkumona yhteiseurooppalaisesta ihanteesta yksilönvapaudesta ja sen heijastumisesta lainsäädäntöön. Näin vahvasti yksityistä kuluttajaa suosiva lainsäädäntö ei ole yleismaailmallinen oikeus, ja Eurooppa

onkin ottanut erilaisen lähtökohdan verrattuna esimerkiksi Yhdysvaltoihin tai lukuisiin Aasian maihin. Tietosuojalakien päivitys on kuitenkin ollut vahvasti esillä eripuolella maailmaa ja joissain tapauksissa mallia on otettu suoraan Euroopan yleisestä tietosuoja-asetuksesta. Yhtenä esimerkkinä voidaan pitää Brasiliaan vuonna 2018 käyttöön otettua yleistä tietojenkäsittelylakia, Lei Geral de Proteção de Dados, LGPD. Se on vahvasti samansuuntainen eurooppalaisen kanssa erityisesti yksityisen kuluttajan oikeuksien osalta. (GDPR.EU 2020.)

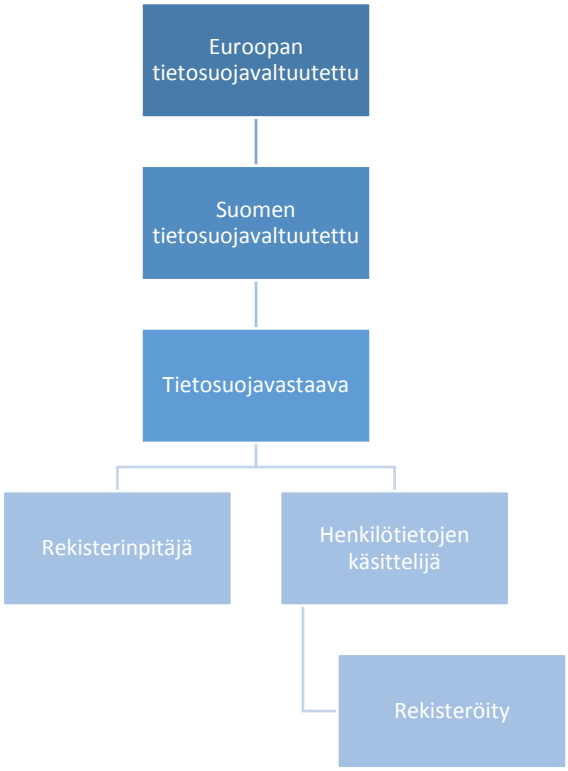
3.2 Tietosuoja-asetuksen vastaanotto

Tietosuoja-asetuksen esittely vuonna 2016 ja sen implementointi vuonna 2018 toi yritykselle valtavan määrän lisätyötä, ja kahden vuoden siirtymäaika on varsinkin jälkikäteen tarkasteltuna ollut hyvin tiukka aikaikkuna. Jokaisen yrityksen tuli käydä läpi talletetut henkilötiedot, asettaa ne tietosuoja-asetuksen velvoittamalle tasolle, ottaa selvää omista vastuista ja velvollisuuksista sekä dokumentoida prosessi ja toimenpiteet. Tämä toi mukanaan uusia rooleja ja vastuita yritysten sisällä, sekä valtavat määrät työtä joka meni yritysten ydintoiminnan ulkopuolelle.

Työmäärästä johtuen ei yleisen tietosuoja-asetuksen vastaanotto ollut pelkästään positiivista, vaan kriittisiä puheenvuoroja käytiin erityisesti median välityksellä, ja varsinkin isot Yhdysvaltalaiset yritykset painottivat omia näkemyksiään asetuksen tärkeydestä ja lopullisesta hinnasta. On arvioitu, että tietosuoja-asetuksen implementointi tuona kahden vuoden siirtymäaikana aiheutti 500 suurimmalle globaalille yritykselle noin 7 miljardin euron menoerän. (Khan 2017.) Riippumatta lopullisesti hinnasta, jotain työn määrästä kertoo se, että esimerkiksi Microsoftilla GDPR -asetus sitoi 1600 insinööriä työskentelemään suoraan asetusten asettamien velvollisuuksien eteen. (Brill 2018.)

Jotkut Yhdysvaltalaiset yritykset myös suoraan kieltäytyivät asetusten asettamista velvollisuuksista ja näin ollen valitsivat olla palvelematta Eurooppalaisia asiakkaita ja kuluttajia tietosuoja-asetukseen vedoten. (Kuchler 2018.)

Tietosuoja-asetuksen toimeenpanoa ja seurantaa valvovat erilliset valvontaviranomaiset kussakin jäsenvaltiossa, ja mikäli toimintaa löytyy usean jäsenvaltion alueelle, on tapana toimia yrityksen päätoimipaikan lainsäädännön mukaisesti. Suomessa henkilötietojen käsittelyä valvoo Suomen tietosuojavaltuutettu, joka johtaa ja on osana tietosuojavaltuutetun toimistoa. Euroopan unionin ylimpänä valvovana elimenä toimii Euroopan tietosuojavaltuutettu. Tämän vastuulla on suorittaa erilaisia selvityksiä, sekä valvoa että EU:n oma hallinto toimii tietosuoja-asetuksen mukaisesti. Alla oleva kuvio 2 selventää vastuuhierarkian kuluttajasta ylimpään valvovaan elimeen.



Kuvio 2. Tietosuoja-asetuksen valvonnan pelkistetty vastuuhierarkia

Tietosuoja-asetuksen toimeenpanon myötä yritysmaailma on joutunut nopealla aikataululla läpikäymään asiakasrajapinnan ja siihen liittyvän tiedonkeruun ja tietojen tallentamisen. Lisäksi isoissa yrityksissä on myös jouduttu järjestämään prosesseja uudelleen, sillä tietosuoja-asetus koskee myös sisäisiä prosesseja, vaikka henkilötietoja kerättäisiinkin vain yrityksen sisäisiin tarpeisiin. Tämä on tarkoittanut uusien roolien esiin kasvamista sekä uusien vastuiden määrittelyä ja jakoa.

3.3 Seloste käsittelytoiminnasta

Yksi yleisen tietosuoja-asetuksen kulmakivistä on seloste käsittelytoiminnasta. Se tulee tehdä, jos organisaatiossa on yli 250 työntekijää, tai jos henkilötietojen käsittely ei ole satunnaista tai sillä voidaan aiheuttaa rekisteröidylle vahinkoa tai oikeuksien tai vapauksien menetyksiä. (Tietosuojavaltuutetun toimisto 2019c.) Seloste käsittelytoiminnasta on osa osoitusvelvollisuuden toteutumista, ja se osoittaa omalta osaltaan, että henkilötietoja käsitellään tietosuojalainsäädännön mukaisesti. Seloste on tarkoitettu vain organisaation omaan käyttöön, mutta se on tarvittaessa pystyttävä toimittamaan valvontaviranomaisille jotka pystyvät tämän perusteella arvioimaan henkilötietojen käsittelyn lainmukaisuutta. Seloste käsittelytoiminnasta tulee tehdä erikseen sekä rekisterinpitäjälle että henkilötietojen käsittelijälle. Tietosuojavaltuutetun toimisto tarjoaa selosteiden toteuttamiseen erinomaiset mallit, mutta tarvittaessa selosteen voi tehdä hyväksi katsomallaan tavalla, kunhan tarvittavat tiedot käyvät selosteesta ilmi.

Tietosuojavaltuutetun toimisto velvoittaa että rekisterinpitäjän vaatimassa selostuksessa on seuraavat tiedot: (Tietosuojavaltuutetun toimisto 2019d)

- Rekisterinpitäjän ja tietosuojavastaavan yhteystiedot ja nimi
- Henkilötietojen käsittelyn tarkoitus
- Kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
- Ryhmät, joille henkilötietoja on luovutettu tai luovutetaan
- Tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainvälisille järjestöille
- Tietojen säilytysajat
- Kuvaus teknisistä ja organisatorisista turvatoimista

Tietosuojavaltuutetun toimisto velvoittaa että henkilötietojen käsittelijän selosteesta löytyy seuraavat tiedot: (Tietosuojavaltuutetun toimisto 2019e)

- Käsittelijän ja tietosuojavastaavan yhteystiedot
- Rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät
- Tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle
- Kuvaus teknisistä ja organisatorisista turvatoimista

3.4 Tietosuojavastaava

Tietosuojavastaavan rooli laajeni yleisen tietosuoja-asetuksen voimaantullessa vuonna 2018 kaikkiin yrityksiin, järjestöihin ja erilaisiin julkisiin hallintoihin. Tätä ennen tietosuojavastaavat ovat olleet pakollisia vain sosiaali- ja terveysalalla. Yleisen tietosuoja-asetuksen mukaan tietosuojavastaavan nimittäminen toimivaan yritykseen on pakollista kolmessa tapauksessa, 37 artiklan 1 kohta: (Elinkeinoelämän keskusliitto 2020)

- Tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin (riippumatta siitä, mitä tietoja käsitellään)
- Rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
- Rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisesti henkilötietoryhmiin tai rikostuomiota tai rikkomuksia koskeviin tietoihin

Tietosuojavastaavan rooliin on muutamia estäviä tekijöitä, jotka on käsiteltävä firman sisäisesti tapauskohtaisesti. Tietosuojavastaavalla ei saa olla eturistiriitoja tietosuojavastaavan tehtävien kanssa, eikä tietosuojavastaava saa lähtökohtaisesti olla määrittämässä henkilötie-

tojen käsittelyn tarkoitusta tai keinoja niiden käsittelyn toteutumiseen (Tietosuojavaltuutetun toimisto 2019f).

Kun yritys on valinnut tietosuojavastaavan, on tämän yhteystiedot lähetettävä tietosuojavaltuutetun toimistolle. Tietosuojavastaavan yhteystietojen on myös oltava organisaation sisäisesti helposti saatavilla ja vastuut selvillä. Lisäksi yrityksen ulkopuolisten rekisteröityjen tulee saada tietosuojavastaavan yhteystiedot helposti esille esimerkiksi yrityksen nettisivuilta.

Mikäli yrityksen ei tarvitse nimetä tietosuojavastaavaa, eikä siihen ryhdytä vapaaehtoisuudenkaan perusteella, tulee yrityksen silti tehdä selvitys kuka on tietosuoja-asetuksen noudattamista valvova henkilö, dokumentoida se ja viestittävä selkeästi sekä sisäisille että ulkoisille sidosryhmille, sen mukaan keiden on tarpeellista olla tästä tietoisia.

Tietosuojavastaavan tärkeimpinä tehtävinä organisaatiossa on valvoa tietosuoja-asetuksen ja tietosuojasääntöjen noudattamista. Tietosuojavastaavan tulee olla selvillä miten organisaatiossa käsitellään henkilötietoja ja hänen tulee olla tukena ja apuna henkilötietoja käsitteleville työntekijöille ja johdolle. Lisäksi tietosuojavastaava on vastuussa, yhdessä rekisterinpitäjän kanssa, henkilötietojen käsittelyyn osallistuvan henkilöstön koulutuksesta ja pitämisessä tiedoiltaan ja taidoiltaan ajan tasalla. Tietosuojavastaava toimii myös yhteyshenkilönä niin valvontaviranomaisiin kuin rekisteröityihin kaikissa henkilötietojen käsittelyyn liittyvissä asioissa. Tietosuojavastaavan rooliin ei ole määritelty erillistä ammattipätevyyttä tai vaatimuksia koulutustasosta. Tietosuojavastaavan on kuitenkin oltava tietoinen kunkin liiketalousalan erityispiirteistä, tunnettava Euroopan unionin asettama yleinen tietosuoja-asetus ja oltava tietoinen kansallisesta lainsäädännöstä. Tietosuojavastaavan vastuu korostuu myös organisaation tietosuojakulttuurin edistäjänä ja oman ammattitaidon ja pätevyyden jatkuva päivittäminen onkin olennainen osa tietosuojavastaavan ammattikuvaa. On kuitenkin huomattava, että vastuu tietosuoja-asetuksen noudattamisesta on aina yrityksellä, eikä vastuuta voi vierittää kokonaisuudessaan tietosuojavastaavan päälle. Mikään ei estä tietosuojavastaavan nimeämistä myös tilanteissa missä sitä ei varsinaisesti vaadita, ja tietosuojavaltuutetun toimisto kannustaakin pyrkimään siihen myös vaikka edellä mainitut kohdat eivät täyttyisikään. Tietosuojavastaavan nimeäminen vapaaehtoisesti ei muuta vastuuta, vaan vapaaehtoisesti nimetyllä tietosuojavastaavalla vastuut ovat samanlaiset kuin tilanteessa missä nimeäminen on pakollista (Tietosuojavaltuutetun toimisto 2019m; Tietosuojavaltuutetun toimisto 2019f).

On yrityksen päätettävissä palkataanko tietosuojavastaava yrityksen ulkopuolelta sopimusperusteella, vai onko tietosuojavastaava suoraan yrityksen työntekijä. Niissä tapauksissa missä tietosuojavastaavaa ei ole pakollista nimetä, eikä siihen lähdetä vapaaehtoisuudenkaan nimissä, voi tietosuoja-asetusta valvova taho hoitaa sivutoimisesti tietosuoja-asioita. On otettava myös huomioon että tietosuojavastaava pitää olla koko ajan tavoitettavissa, eli organisaation

on järjestettävä sijainen joka hoitaa tehtäviä varsinaisen tietosuojavastaavan loma-aikoina tai muiden poissaolojen tapauksissa.

3.5 Henkilötietojenkäsittelijä ja rekisterinpitäjä

Muita tietosuoja-asetukseen läheisesti liittyviä rooleja tietosuojavastaavan ohella ovat rekisterinpitäjä ja henkilötietojen käsittelijä. Rekisterinpitäjällä tarkoitetaan yleensä yritystä, toimijaa tai julkista hallintoa, joka on määritellyt henkilötietojen käsittelyn tarpeen sekä keinot niiden käsittelyyn. Henkilötietojen käsittelijällä tarkoitetaan henkilöä tai toimijaa joka toimii rekisterinpitäjän alaisuudessa ja sen ohjeiden mukaisesti. Henkilötietojen käsittelijällä ei kuitenkaan tarkoiteta rekisterinpitäjän työntekijää, joka osana omaa työtään käsittelee henkilötietoja. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 24).

3.5.1 Henkilötietojen käsittelijä

Henkilötietojen käsittelijä asettuu tietosuoja-asetuksen velvollisuuksien piiriin kun sen toiminta on sijoittunut Euroopan unionin jäsenvaltioon, tai EU:n ulkopuoliseen toimijaan jonka palvelut tai muut toiminnat vaativat Euroopan unionin jäsenvaltojen alueelle rekisteröityjen henkilötietojen käsittelyä. Tietosuoja-asetus säätää erikseen velvollisuudet henkilötietojen käsittelijöille. Yhteistyö rekisterinpitäjän kanssa velvoittaa henkilötietojen käsittelijän auttamaan ja neuvomaan rekisterinpitäjää tietosuoja-asetuksen määrittämien velvollisuuksien täyttymisessä. Lisäksi velvollisuuksiin luetaan ilmoitukset henkilötietojen loukkauksista, tietosuojaa koskevat vaikutustenarvioinnit, yleinen tietoturva, koulutuksiin ja auditointeihin osallistuminen ja tarvittaessa rekisteröityjen tietojen tuhoaminen. (Tietosuojavaltuutetun toimisto 2019g).

Yksi tärkeimmistä asioista henkilötietojen käsittelijän roolissa on tietojen jäljitettävyys. Tietojenkäsittelytoimisto on antanut seuraavat ohjeistukset sen toteutumiseen, missä henkilötietojen käsittelijän täytyy: (Tietosuojavaltuutetun toimisto 2019h)

- Laatia rekisterinpitäjän kanssa sopimus tai muu oikeudellinen asiakirja, jossa määritellään kunkin osapuolen velvollisuudet ja joka kattaa tietosuoja -asetuksen 28 artiklan edellyttämän tietosisällön.
- Laatia rekisterinpitäjän antamista henkilötietojen käsittelystä määrittävistä ohjeista kirjallinen luettelo. Käsittelijä voi osoittaa toimivansa rekisterinpitäjän antamien ohjeiden mukaisesti muun muassa tällaisen dokumentoinnin avulla.
- Pyytää rekisterinpitäjältä kirjallinen lupa muiden käsittelijöiden käyttämiseen rekisterinpitäjän henkilötietojen käsittelyssä.
- Toimittaa rekisterinpitäjälle kaikki tiedot, joita tarvitaan velvoitteiden täyttymisen osoittamiseen ja auditointien suorittamiseen.
- Laatia tarvittaessa seloste käsittelytoiminnasta.

3.5.2 Rekisterinpitäjä

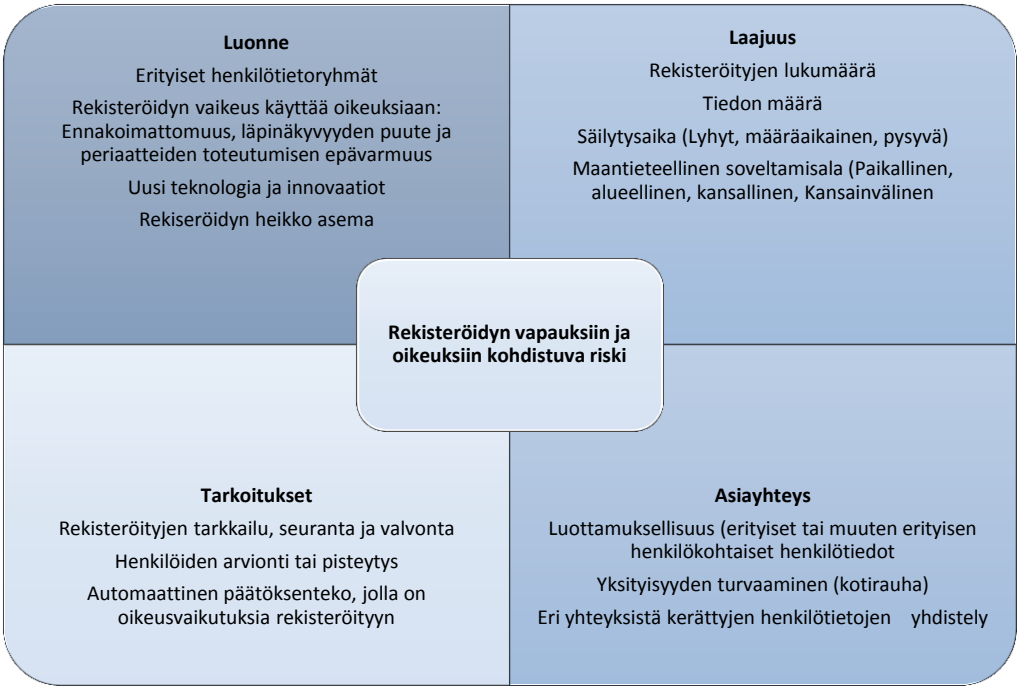
Rekisterinpitäjä on määritelmällisesti yritys, toimija tai julkinen hallinto mikä määrittelee henkilötietojen käsittelyn tarpeen. Ennen henkilötietojen keräämistä rekisterinpitäjän on suoritettava riskien arviointi ja suunniteltava toimenpiteet tietosuojaperiaatteiden toteutumisen varmistamiseksi. Riskien arviointi on tehtävä rekisteröidyn näkökulmasta, eli rekisterinpitäjän tulee varmistaa että rekisteröidyn vapauksia ja oikeuksia ei vaaranneta tarpeettomasti. Tässä arvioinnissa tulee myös selvittää etukäteen mitä vahinkoa rekisteröidylle voi aiheutua henkilötietojen käsittelystä.

3.6 Riskien arviointi

Riskien arvioinnissa on lähdettävä liikkeelle rekisteröidyn näkökulmasta.

- Mitä riskejä henkilötietojen käsittely voi aiheuttaa?
- Mitä vahinkoa riskien toteutuminen aiheuttaa rekisteröidylle?

Tässä vaiheessa oleellisinta on, että rekisterinpitäjä on selkeästi tietoinen omasta henkilötietojen käsittelyn tarpeesta. Käsittelyn tarvetta helpottamaan tietosuojavaltuutetun toimisto tarjoaa alla olevaa kaaviota, kuvio 3.



Kuvio 3. Riskien määrittely. (Tietosuojavaltuutetun toimisto 2019i.)

Kun riskit ja niistä mahdollisesti aiheutuvat haitat on tunnistettu, tulee pohtia haittojen vakavuutta ja niiden toteutumisen todennäköisyyttä. Riskien arvioinnissa voidaan käyttää apuna

riskianalyysitaulukkoa. Tietosuojavaltuutetun toimisto tarjoaa tähän mallipohjan, alta löytyvä kuvio 4.

Loukkauksen tai haitan vakavuus	Vakava	Matala riski	Korkea riski	Korkea riski
	Tunnistettuja vaikutuksia	Matala riski	Keskimääräinen riski	Korkea riski
	Vähäisiä vaikutuksia	Matala riski	Matala riski	Matala riski
		Kaukainen	Mahdollinen	Hyvin mahdollinen
		Loukkauksen tai haitan todennäköisyys		

Kuvio 4. Riskimatriisi (Tietosuojavaltuutetun toimisto 2019i.)

Riskien analysoinnissa ja tunnistamisessa on otettava huomioon, ettei se ole vain kertaluontoinen projekti, vaan on tunnistettava organisaatiossa tapahtuvat muutokset, muutokset toimintatavoissa tai muutokset tekniikassa jotka vaativat riskien uudelleenanalysointia. Rekisterinpitäjällä on osoitusvelvollisuus myös siitä, että riskejä lähestytään analyyttisesti ja ne on otettu jo suunnitteluvaiheessa huomioon.

Mikäli riskianalysointi osoittaa korkeaa riskiluokkaa rekisteröidyn vapaudelle tai oikeuksille, on rekisterinpitäjä velvoitettu tekemään vaikutuksenarvioinnin omista toiminnoistaan. Suomen tietosuojavaltuutetun toimisto kehottaa käyttämään vaikutuksen arviointia muutoinkin kuin pakkotilanteessa, sillä tällä voidaan hyvin dokumentoida henkilötietojen käsittelyn suunnittelua ja perustella ratkaisuja jälkikäteen, mikäli tarvetta tulee.

3.7 Vaikutustenarviointi, osoitusvelvollisuus ja auditointi

Vaikutustenarviointi (DPIA) on pakollista jos riskianalyysi paljastaa korkean mahdollisuuden ihmisten oikeuksien tai vapauksien loukkauksiin. (Tietosuojavaltuutetun toimisto 2019j.) Rekisterinpitäjä voi käyttää vaikutustenarviointia apunaan, vaikka riskit eivät nousisikaan korkeimpaan luokkaan, sillä vaikutustenarvioinnista on apua riskien tunnistamisessa ja niiden hallitsemisessa. Vaikutustenarvioinnin lopullisena tarkoituksena on selvittää onko analyysissä ja arvioinnissa selvinneiden riskien ottaminen oikeutettua. Lisäksi vaikutustenarviointi on apuna lainsäädännön noudattamisessa, sekä toimii apuna dokumentoinnissa ja osoitusvelvollisuuden toimeenpanossa. Mikäli yrityksen tai toimijan riskit muuttuvat ajan myötä, tulee vaikutustenarviointia päivittää asianmukaisesti. Useasti päivitysten tarve tulee esimerkiksi uuden tekniikan käyttöönotossa.

Rekisterinpitäjä tekee vaikutustenarvioinnin yhdessä tietosuojavastaavan kanssa, mikäli tietosuojavastaava on nimitettynä. Lisäksi henkilötietojen käsittelijällä on velvollisuus toimia apuna arvioinnissa, mikäli tämän apua tarvitaan.

Osoitusvelvollisuus tarkoittaa rekisterinpitäjän velvollisuutta pystyä näyttämään toteen tietosuoja-asetuksen toimeenpanon onnistuminen. Osoitusvelvollisuus vaatii rekisterinpitäjältä onnistuneita esitoimia riskien analysoinnissa, sekä analysoinnin, ja tarvittaessa myös vaikutusten arvioinnin dokumentointia. Jos henkilötietojen käsittelyssä arvioitu riski toteutuu, pystyy rekisterinpitäjä dokumentoinnin ja osoitusvelvollisuuden avulla näyttämään toteen, että riskit on tunnistettu, ne on todettu oikeutetuiksi, sekä niiden minimoimiseksi ovat tehty tarvittavat toimenpiteet.

Tietosuoja-asetuksessa on määritelty osoitusvelvollisuuksia koskevia vaatimuksia, mutta näiden velvoittavuus on tarkasteltava tapauskohtaisesti, riippuen esimerkiksi organisaation koosta, henkilötietojen määrästä, millaista dataa rekisterinpitäjä käsittelee jne. (Tietosuojavaltuutetun toimisto 2019k.) Oleellista on että rekisterinpitäjä ottaa osoitusvelvollisuuden huomioon jo suunnittelu- ja riskienkartoitusvaiheessa.

Yritysten avuksi on tarjolla myös kolmannen osapuolen järjestämiä auditointeja, joilla voidaan selvittää toimintatapoja, tietosuoja-asetuksen toimeenpanoa, saada yleisnäkymää organisaatiosta , toteuttaa osoitusvelvollisuutta sekä löytää mahdollisia korjaustoimenpiteitä.

3.8 Mahdolliset tietoturvaloukkaukset

Tietosuojavaltuutetun toimisto määrittelee tietoturvaloukkaukset seuraavasti "Henkilön tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta." (Tietosuojavaltuutetun toimisto 2019l.)

Tietosuoja-asetuksen velvoittaman käsittelyjärjestyksen mukaan kaikki tietoturvaloukkaukset tulee dokumentoida ja korjaavat toimenpiteet tulee tehdä riippumatta siitä mikä tietoturvaloukkauksen lopullinen haitta on. Sekä tietoturvaloukkaus että siitä seuraavat korjaukset tulee dokumentoida.

Tietosuoja-asetuksen asettamien velvollisuuksien noudattamatta jättäminen on rangaistuksen arvoinen teko. Tietosuojaviranomainen voi käyttää valtuuksiaan tällaisissa tapauksissa ja määrätä toimijalle huomautuksia, tai väliaikaisia ja jopa pysyviä käsittelykieltoja. Viimeisimpänä toimenpiteenä voi valvontaviranomainen määrätä hallinnollisen sakkorangaistuksen, joka rikkomuksen vakavuudesta riippuen voi olla jopa 10-20 miljoonaa euroa tai 2 % -4 % edellisen tilivuoden maailmanlaajuisesta liikevaihdosta, riippuen siitä kumpi näistä määristä on suurempi.

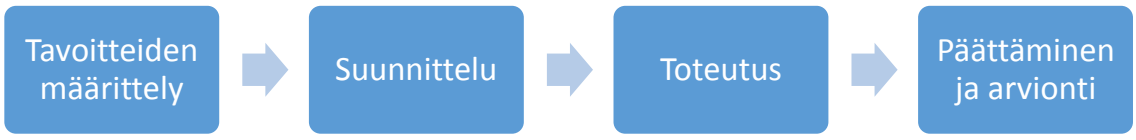
4 Tutkimus ja kehittämismenetelmät

Tämän opinnäytetyö on luonteeltaan tutkimuksellisen kehitystyö. Tutkimuksellista kehittämistoimintaa voidaan pitää yleiskäsitteenä, jolla kuvataan tutkimustoiminnan ja kehittämistoiminnan yhteyttä, ja sitä miten tutkimuksen perusteella löydettyä tietoa voidaan käyttää konkreettisen kehittämisen apuna (Toikko & Rantanen 2009, 19-21).Tässä työssä menetelmällä on etsitty aineistotutkimuksen perusteella konkreettista kehitystoimintaa tutkimuskysymyksen ympärille.

Työn teoreettiseen osuuden tavoitteena oli rakentaa kokonaiskuvaa laajasta aihepiiristä ja kuvata tietosuoja-asetusta erityisesti aloittavan yrityksen näkökulmasta. Tarkoitus oli perehtyä mahdollisimman spesifiin, mutta kuitenkin tarpeeksi useaan kirjalliseen lähteeseen, jolla haettiin vastausta tutkimuskysymykseen asiakasyrityksen toimintojen ja vastuumäärittelyiden asettamisesta tietosuoja-asetuksen laajempaan kontekstiin. Tietoa on hankittu painetusta kirjallisuudesta ja tietosuojavaltuutetun sivuilta. Tiedonhankintaa on pääosin rajoitettu koskemaan vain suomenkielistä materiaalia, sillä verkkokaupan toimintaympäristö on Suomi, ja vaikka tietosuoja-asetus onkin yleiseurooppalainen säädös, on validiteetin kannalta oleellista että käytetään toimintamaan lainsäädännön mukaista ohjeistusta.

Työn toiminnallisen osuuden tarkoituksena oli siis tuottaa yritykselle tarpeellinen materiaali, jolla varmistaa tietosuoja-asetuksen tärkeimpien asioiden ymmärtäminen ja implementointi. Tätä lähtökohtaa vasten tarkka aineiston valinta on ollut oleellisena asian työn onnistumisen kannalta. Lähdekritiikkiin nojaten aineisto on valittu painetusta kirjallisuudesta ja muutamista luotettavista verkkoartikkeleista. Sähköisistä lähteistä erityisesti tietosuojavaltuutetun toimisto on määritelty luotettavaksi lähteeksi, sen ollessa Suomen korkein auktoriteetti tietosuoja-asetuksen saralla ja sen toimiessa valvovana viranomaisena.

Työn kehittämistoiminnallinen osuus on seurannut ns. lineaarista kehittämisprosessin mallia, missä prosessin eteneminen voidaan pelkistää yksinkertaisiin vaiheisiin: tavoitteiden määrittely, suunnittelu, toteutus ja päättäminen. (Toikko & Rantanen 2009, 64.)Tavoitteiden määrittely ja suunnittelu -vaiheet kävivät läpi muutaman iteraation ennen lopullista muotoutumista ja toteutukseen ja päättämiseen saapumista. Projektityön lineaarinen malli voidaan rakentaa alla olevan kuvio 5 mukaisesti.

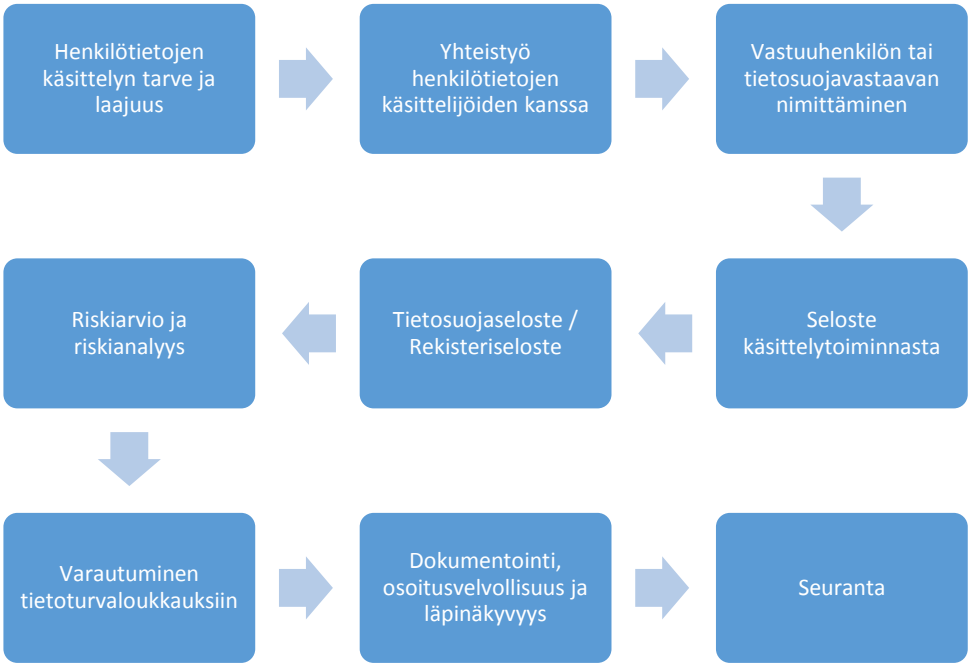


Kuvio 5 Projektityön lineaarinen malli (Toikko & Rantanen 2009,64.)

5 Ohjeistus asiakasyritykselle

Asiakasyritys käy verkkokauppaa vain myyntitarkoitukseen, ostotoimintoja samaan verkkoalustaan ei ole tarkoitus rakentaa. Yrityksen verkkokauppa-alusta tilataan kolmannelta osapuolelta ja asiakasyrityksen roolina tulee olemaan rekisterinpitäjä. Verkkokauppa-alustan ylläpitäjä toimii henkilötietojen käsittelijän roolissa. Asiakasyritys tulee tekemään henkilötietojen käsittelijöiden kanssa tarkemmat sopimukset sekä vastuiden määrittelyt erikseen, alla olevaa listausta käytetään eräänlaisena oleellisimpien asioiden muistilistana täydentämään muita tietolähteitä.

Yrityksen avuksi rakennettu muistilista on typistetty mahdollisimman lyhyeksi ja se sisältää yhdeksän kohtaa. Nämä kohdat ovat valikoitu mukaan siitä lähtökohdasta, mitä yrityksen tulee ottaa huomioon, tai olla vähintään tietoinen, toimintoja ylös nostaessa. Listaus ei ole siis täysin kattava otos tietosuoja-asetuksesta, vain tärkeimmät asiat aloituksen tueksi. Listauksessa mennään suurpiirteisessä aikajärjestyksessä, mutta oleellisinta on kaikkien kohtien ymmärtäminen ja reagoiminen oikeilla toimenpiteillä, ei niinkään suoritusjärjestys. Alla olevassa kuviossa 5 on tiivistetty muistilistan sisältö eri vaiheineen ja tässä pääluvussa käydään kohtia tarkemmin läpi.



Kuvio 6. Yhdeksän tärkeintä kohtaa asiakasyritykselle

5.1 Rekisteröidyn oikeudet

Kaikessa henkilötietojen käsittelyssä on otettava huomioon tietosuoja-asetuksen perusajatus rekisteröidyn oikeuksista. Kaikki yrityksen toimet tulee järjestää näitä oikeuksia tukevaksi ja nämä tulee tiedostaa kaikessa toiminnassa. Rekisterinpitäjän tulee toteuttaa kaikki käsillä olevat toimet oikeuksien toteutumiseksi ja sen on osaltaan helpotettava rekisteröidyn ymmärrystä oikeuksistaan, pääsyä niihin käsiksi ja autettava tarvittaessa rekisteröityä käyttämään oikeuksiaan. Rekisteröidyn oikeudet muuttuvat hiukan käsittelyperusteen mukaan. Verkkokaupan käsittelyperusteena sopimus ja suostumus, sopimus solmitaan asiakassuhteen mukana ja suostumus erikseen kysyttäessä.

Tietosuoja-asetuksen mukaan rekisteröidyn tärkeimmät oikeudet kun käsittelyperusteena on suostumus tai sopimus: (Tietosuojavaltuutetun toimisto 2019n)

- Saada tietoa henkilötietojen käsittelystä
- Saada pääsy tietoihin
- Oikaista tietoja
- Poistaa tiedot tai tulla unohdetuksi
- Rajoittaa tietojen käsittelyä
- Siirtää tiedot järjestelmästä toiseen
- Vastustaa tietojen käsittelyä
- Olla joutumatta automaattisen päätöksenteon kohteeksi

Lisäksi suostumuksellisessa käsittelyperusteessa rekisteröidyllä on oikeus sallia automaattisen päätöksenteon nimenomaisella aktiivisella suostumuksellaan. Tätä voi hyödyntää esimerkiksi erilaisissa profiloinneissa.

5.2 Rekisterinpitäjän selvitys kerättävistä henkilötiedoista

Tietosuoja-asetuksen velvoitteiden käyttöönotossa on tarkoituksenmukaista lähteä liikkeelle omasta tarpeesta henkilötietojen käsittelyyn ja näiden tarpeiden perusteluista. Mitä henkilötietoja on pakko kerätä oleellisena osana yritystoimintaa ja mitä henkilötietoja tullaan käyttämään osana mainontaa tai analytiikkaa. Tietosuoja-asetus määrittelee, että yrityksellä on oikeus kerätä vain tietoa joka on toiminnan kannalta tarpeellista ja tähänkin tarvitaan asiakkaan vapaaehtoinen, tietoinen ja yksiselitteinen suostumus.

On tarpeen koota henkilötietojen keräystarpeet ja merkitä ylös perusteet miksi juuri niitä henkilötietoja on kerättävä. Henkilötietojen keräys on tehtävä pienimmän mahdollisen haitan kautta. Päätökset ja perustelut tulee dokumentoida, joko erikseen tai osaksi selostetta henkilötietojen käsittelystä.

5.3 Yhteistyö henkilötietojen käsittelijän kanssa

Asiakasyrityksen tietosuoja-asetuksen määrittämä rooli tulee olemaan rekisterinpitäjä. Rekisterinpitäjän tulee luoda toimeksiannot henkilötietojen käsittelijöiden suuntaan, eli esimerkiksi verkkokaupan verkkoalustan toteuttajalle, eli taholle joka varsinaisesti käsittelee, tallentaa ja säilyttää henkilötietoja, sekä esimerkiksi sähköpostimarkkinointia hoitavalle yritykselle. Jokaisen toimeksiannon kanssa on huolehdittava että tietosuoja-asetus on otettu huomioon kaikessa toiminnassa ja tarvittavat sopimukset on tehty vastuut määritellen.

Vaikka varsinainen henkilötietojen käsittely on ulkoistettu henkilötietojen käsittelijälle, on otettava huomioon että rekisterien vastuuta ei voi ulkoistaa, vaan lopullinen vastuu tietojen käsittelystä säilyy aina rekisterinpitäjän harteilla. Sopimukset ja vastuiden määrittelyt tulee dokumentoida asianmukaisesti.

5.4 Seloste käsittelytoiminnasta

Seloste käsittelytoiminnasta on erinomainen asiakirja yrityksen sisäiseen dokumentaatioon ja henkilötietojen käsittelyn hahmottamiseen. Lisäksi se toimii osaltaan osoitusvelvollisuuden näyttämisestä toteen. Vaikka seloste on tarkoitettu vain organisaation sisäiseksi asiakirjaksi, on seloste tarvittaessa pystyttävä toimittamaan valvontaviranomaisille.

Tietosuojavaltuutetun toimisto tarjoaa kaksi erilaista mallipohjaa selosteeksi käsittelytoiminnasta, toinen henkilötietojen käsittelijälle, toinen rekisterinpitäjälle. Näitä mallipohjia voidaan käyttää osana kuvaamaan henkilötietojen käsittelytoimien vastuita, mutta tarvittaessa

selosteen voi laatia itsekin, kunhan asiakirjasta löytyy tarvittavat tiedot. Tietosuojatoimiston mukaan rekisterinpitäjän selosteessa tulisi olla mainittuna ainakin seuraavat seikat:

- Rekisterinpitäjän yhteystiedot
- Tietosuojavastaavan, tai vastuullisen yhteystiedot
- Mihin tarkoitukseen tietoja kerätään?
- Rekisteröityjen ryhmät?
    - Verkkokaupan tapauksessa ryhmä: asiakkaat
- Mitä tietoja kerätään?
- Vastaanottajaryhmät?
- Viittaus henkilötietojen käsittelijän kanssa solmittuun sopimukseen
- Tieto siitä ettei henkilötietoja siirretä kolmansiin maihin tai kansainvälisiin järjestöihin
- Tietojen säilytysajat
- Kuvaus tietosuoja-asetuksen 32 artiklan 1 kohdan mukaisista teknisistä ja organisatorisista turvatoimista.
    - Esimerkiksi miten tiedot suojattu yrityksen ulkopuolisilta, miten käyttöoikeus rajattu organisaation sisällä

Rekisterinpitäjä voi liittää omaan selosteeseensa henkilötietojen käsittelijän laatiman selosteen ja käyttää tätä osana vastuiden määrittelyä. Seloste käsittelytoiminnasta tulee dokumentoida hyvin ja säilyttää saatavilla.

5.5 Tietosuojaseloste ja rekisteriseloste

Tietosuojaseloste on tarkoitettu ensisijaisesti rekisteröidyn oikeuteen tietää mitä tietoja tallennetaan, mihin niitä käytetään, miten saada selville mitä tietoja henkilöstä on tallennettu ja miten niitä voidaan pyynnöstä muokata tai poistaa. Tietosuojaseloste tulee olla selkeästi näkyvillä verkkosivuilla ja sen tulee olla mahdollisimman helposti luettavissa ja selkeästi kirjoitettu. Tämä kannattaa tehdä yhteistyössä verkkokaupan palveluntarjoajan kanssa.

Tietosuojaselosteessa tulee olla selvillä ainakin seuraavat asiat:

- Rekisterinpitäjä ja yhteystiedot
- Tietosuojavastaava, jos löytyy, ja yhteystiedot
- Rekisterin käyttötarkoitus
- Tietojen keräämisen peruste
- Tietojen säilytysaika
- Tietojen luovutus
- Rekisterin suojaus

- Evästeiden käyttö
- Rekisteröidyn oikeudet

Tietosuojaseloste toimii rekisteröidylle myös luottamuslauseena verkkokaupan tietosuoja-asetuksen velvoittamia toimia kohtaan. Tämä on tehtävä huolella ja samalla on huolehdittava toimien läpinäkyvyydestä sekä yksiselitteisyydestä.

5.6 Sähköpostimarkkinointi

Sähköpostimarkkinoinnin oletetaan tapahtuvan ulkopuolisen palveluntarjoajan avulla. Tämä tarkoittaa rekisterinpitäjän kannalta uusia sopimuksia ja määrittelyjä palveluntarjoajan, eli henkilötietojen käsittelijän kanssa. Alla olevat ohjeistukset koskevat suostumukseen perustuvaan henkilötietojen käsittelyä.

Sähköpostilistojen käyttäminen markkinointiin tarvitsee perustella tietosuoja-asetuksen nojalla ja listojen käyttämiseen on löydettävä laillinen oikeusperuste. Eli käytännössä tämä tarkoittaa, että tietosuoja-asetuksen artikla 6 esitettyjen oikeudellisien perusteiden on täytyttävä ainakin yhdeltä kohdalta. Tietosuoja-asetuksen artikla 6 kertoo oikeudelliset perusteet seuraaviksi: (Digiturvamalli 2017)

- Rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten
- Käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä
- Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi
- Käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi
- Käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi
- Käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteutumiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Sähköpostimarkkinointi voidaan perustella artiklan ensimmäisellä kappaleella. Eli jos asiakas antaa suostumuksen henkilötietojen käsittelyyn, voidaan näitä tallentaa tarpeen mukaisesti. Oleellista on siis pyytää asiakkaan suostuminen ja varmistaa että asiakas tietää mihin suostuu. Kaikki valinnat on pystyttävä perustelemaan jälkikäteen osoitusvelvollisuuden nimissä.

Myös sähköpostimarkkinointi on muuttunut yleisen tietosuoja-asetuksen voimaantulon jälkeen enemmän kuluttajaa suosivaksi, sillä missä ennen sähköpostimarkkinointi on perustunut ns. opt-out -periaatteeseen, velvoittaa nykyinen tietosuoja-asetus suoramarkkinoinnin vain suostumuksen antamalla opt-in -periaatteella. Opt-in -periaate siis tarkoittaa hyväksyntää vaativaa, eli asiakkaan on erikseen hyväksyttävä tiettyjen henkilötietojen käyttö mainittuihin tarkoituksiin, kun ennen hyväksyntä on tullut automaattisesti ja kuluttajalle on jätetty vain mahdollisuus jättäytyä pois markkinoinnin parista, eli opt-out.

Tarkoituksenmukainen asiakaskäyttäytyminen verkkokaupan tapauksessa on syöttää opt-in painike tilausta tehdessä, tai erikseen verkkosivuilla asioidessa, niin että suostumus on yksiselitteinen ja niin että kuluttaja saa tarpeeksi yksityiskohtaisen informaation suoramarkkinoinnista. Toinen vaihtoehto hyvälle asiakaskäyttäytymiselle ja tietosuoja-asetuksen vaatimusten täyttymiselle on niin sanottu kaksivaiheinen hyväksyntä. Käytännössä asiakkaan hyväksyntä hoidetaan niin että tilatessaan uutiskirjeen esimerkiksi verkkosivuilta, tulee asiakkaalle vahvistusviesti sähköpostiin ja vasta tähän vastattuaan tulee varmistus listalle siirtymisestä, opt-in on hoidettu siis sähköpostin välityksellä.

Lisäksi on varmistettava että asiakkaalla on aina mahdollisuus poistua sähköpostilistoilta. Tämä hoidetaan parhaiten itse sähköpostiviestissä olevalla opt-out -ilmoituksella. Asiakkaan tulee päästä suoraan sähköpostista poistamaan itsensä markkinointilistalta tai muuttamaan omia tietojaan.

5.7 Riskianalyysit

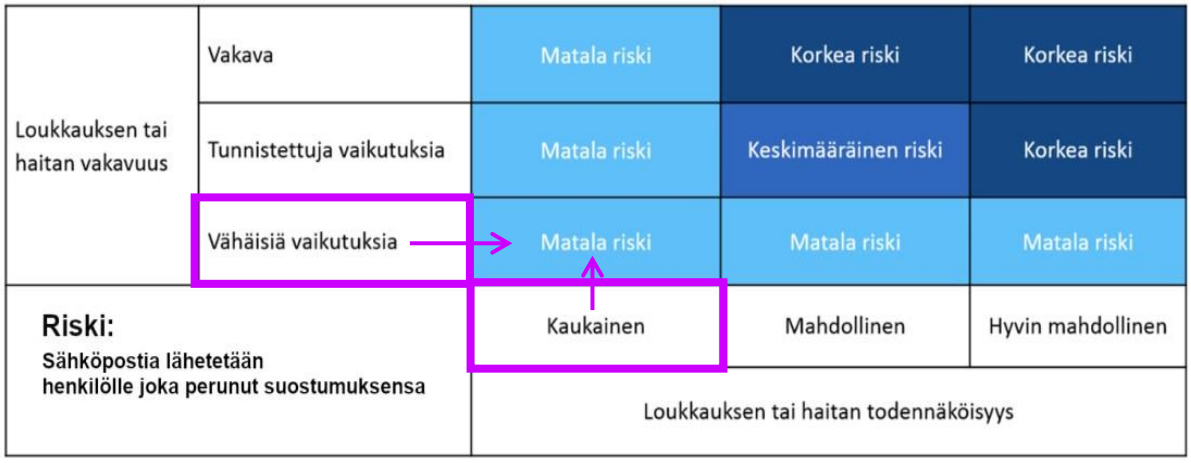
Kaikesta henkilötietojen käsittelystä aiheutuu riskejä rekisteröidylle, ja tätä riskitasoa määrittelemään on tehtävä riskiarviot ja analyysit. Tarkoituksena on tehdä selvyys mahdollisista uhkista ja näiden toteutumisen todennäköisyyksistä. Rekisterinpitäjän tulee tehdä henkilötietojen käsittelijän kanssa vielä yhteiset riskiarviot sekä sopimukset tietojen käsittelystä, mutta seuraavassa kuvataan pääpiirteittäin prosessia jota voidaan käyttää näitä seikkoja tukemaan.

Riskiarvion ensimmäisenä vaiheena on käyttää aiemmin määriteltyä henkilötietojen käsittelyjen tarvetta. Henkilötietoja ei tule käsitellä enempää kuin tarve edellyttää ja tietoja on kerättävä pienimmän mahdollisen käsittelyn periaatteella.

Seuraavassa vaiheessa tulee arvioida riskit rekisteröidyn näkökulmasta. Tällaiset riskit ovat riippuvaisia tallennetuista tiedoista, joten esimerkiksi sähköpostimarkkinoinnissa riskit voivat olla että sähköpostia lähetetään henkilölle joka ei ole antanut suostumusta, sähköpostia lähetetään henkilölle joka on perunut suostumuksensa, sähköpostilistat joutuvat tietomurron kohteeksi tai lähetetystä sähköpostista käy ilmi muiden sähköpostiosoitteita. Riskien arviointi tulee tehdä kattavasti, vaikka riskit olisivatkin lähtökohtaisesti kaukaisia ja epätodennäköisiä. Jos riskit on tunnistettu, riskitasot määritelty ja toimintatavat määritelty näiden mukaan, on

osoitusvelvollisuus onnistunut kokonaisuudessaan kun vielä dokumentointi on hoidettu asianmukaisesti. On otettava huomioon myös se, että jos toimintatavoissa tulee myöhemmin muutoksia, esimerkiksi uusien tekniikoiden tai järjestelmien käyttöönotto, on riskianalyysi tehtävä uudelleen muuttuneilla tiedoilla.

Riskianalyysissä kannattaa käyttää apuna riskimatriisia joka auttaa visualisoimaan riskitasoja ja toimii dokumenttina riskianalyysin osoitusvelvollisuudessa. Yksinkertainen esimerkki riskianalyysin toiminnasta kuviossa 6:



Kuvio 7. Esimerkki riskimatriisin käytöstä

Yllä olevassa kuvassa on määritelty riskiksi markkinointisähköpostin lähettäminen henkilölle joka on käyttänyt peruutusoikeuttaan sähköpostimarkkinoinnista poistumiseen. Arvio haitan vakavuudesta on vaikutukseltaan vähäinen, sillä vaikka se olisi rekisteröidylle vahva epäluottamuslause toiminnan tasosta, ja asianmukaiset selvitykset ja toimintatapojen korjaukset tulisi tehdä rekisteripitäjän ja henkilötietojen käsittelijän toimesta, varsinaiset vaikutukset rekisteröidyn oikeuksiin olisivat varsin vähäiset. Haitan todennäköisyys on arviolta kaukainen. Voidaan olettaa järjestelmien toimivan halutulla tavalla ja näin tämä riski ei pääsisi realisoitumaan. Näin ollen voidaan todeta riskitason olevan matala.

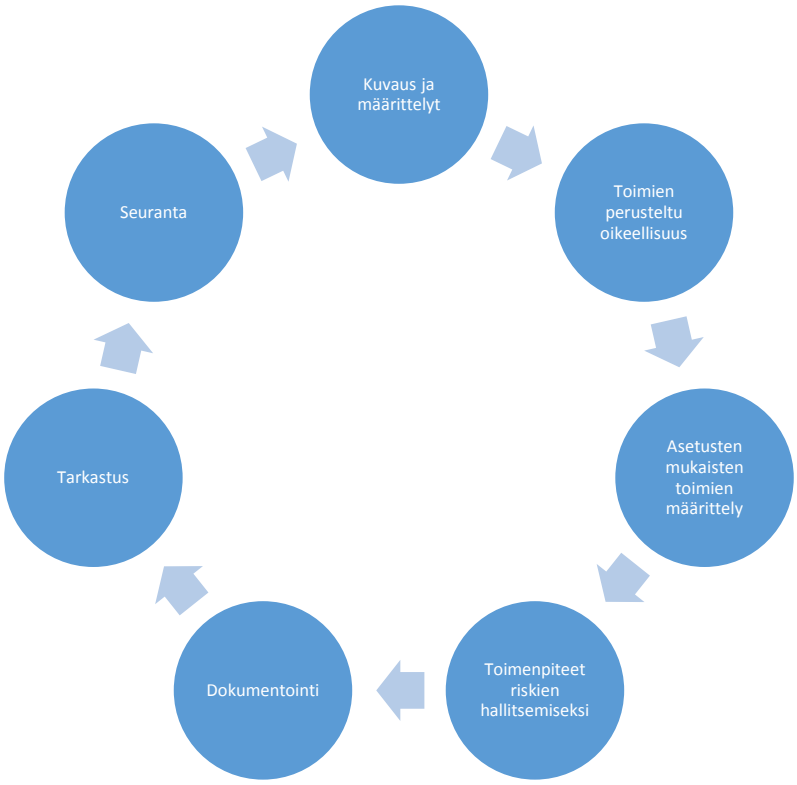
Yllä olevaa periaatetta noudattaen voidaan käydä läpi kaikki löydetyt riskit ja asettaa riskitasot kontekstiin. Riskimatriisit, niiden tulokset ja analyysit tulee dokumentoida osoitusvelvollisuuden onnistumiseksi.

5.8 Osoitusvelvollisuus

Osoitusvelvollisuus tarkoittaa sitä, että rekisterinpitäjän on pystyttävä konkreettisesti osoittamaan että kaikessa toiminnassa noudatetaan tietosuoja-asetuksen säännöksiä ja tietosuojalainsäädäntöä. Lisäksi osoitusvelvollisuus toimii vakuutena siitä, että jos jotain henkilötietoja

päästään jostain syystä loukkaamaan, on käsittelyssä kuitenkin otettu riskit huomioon ja nämä tunnistetut riskit on minimoitu toiminnassa ja kaikki on dokumentoitu asiallisesti.

Toimenpiteeksi muuttaminen voidaan hoitaa alla olevan kaavion, kuvio 8 mukaisesti. Ensimmäisenä tunnistetaan velvollisuudet, eli pitää ymmärtää omat velvollisuudet ja riskit rekisterinpitäjänä sekä henkilötietojen käsittelyn tarpeet. Kun henkilötietojen käsittelyn tarpeet on määritelty, tulee tehdä asianmukainen riskianalyysi. Riskianalyysillä asetetaan henkilötietojen käsittelyn toimet riskejä vastaavaan kontekstiin. Riskianalyysit ja niistä seuraavat toimenpiteet dokumentoidaan ja säilytetään osana osoitusvelvollisuutta. Jos prosessiin tulee muutoksia tulevaisuudessa, esimerkiksi uusien järjestelmien osalta, tulee asianmukaiset riskiarviot tehdä ja dokumentoida uudelleen.



Kuvio 8. Onnistuneen osoitusvelvollisuuden kulmakivet

Osoitusvelvollisuuden onnistumiseksi olennaisinta on dokumentoida henkilötietojen käsittelyn tarve ja suunnitelmat, sopimukset henkilötietojen käsittelijän kanssa, riskiarviot ja riskianalyysit, käytännön toimenpiteet ja varautuminen tietoturvaloukkauksiin.

5.9 Varautuminen tietoturvaloukkauksiin

Osana osoitusvelvollisuuden täyttymistä pitää olla varautunut tietoturvaloukkauksiin ja näiden tapausten varalle on rakennettava toimintasuunnitelma. Tämä voidaan tehdä yhdessä henkilötietojen käsittelijän kanssa, mutta on rekisterinpitäjän vastuulla että näin tulee toimittua.

Toimintasuunnitelman ei tarvitse olla liian yksityiskohtiin menevä, vaan jokaisen tapauksen perusteella arvioidaan erikseen loukkauksen riskit rekisteröidylle. Tämä riskitaso määrittää toimenpiteet mihin rekisterinpitäjän tulee ryhtyä. Jokainen tietoturvaloukkaus tulee dokumentoida yksityiskohtaisesti. Sen jälkeen tulee tehdä korjaavat toimenpiteet ja nämä toimenpiteet tulee myös dokumentoida.

Esimerkkinä toimenpiteitä eri riskitasoille:

- Matala riskitaso: Dokumentoidaan loukkaus. Tehdään korjaavat toimenpiteet. Dokumentoidaan toimenpiteet.
- Kohtuullinen riskitaso: Dokumentoidaan loukkaus. Tehdään korjaavat toimenpiteet. Dokumentoidaan toimenpiteet. Jos rekisteröidyn oikeuksiin tai vapauksiin kohdistuu riskiä ilmoitus valvovalle viranomaiselle 72h sisällä loukkauksesta ja mahdollisesti ilmoitus rekisteröidylle.
- Korkea riskitaso: Dokumentoidaan loukkaus. Tehdään korjaavat toimenpiteet. Dokumentoidaan toimenpiteet. Jos rekisteröidyn oikeuksiin tai vapauksiin kohdistuu merkittävää riskiä ilmoitus valvovalle viranomaiselle 72h sisällä loukkauksesta ja ilmoitus rekisteröidylle.

Toimintaohje tietoturvaloukkauksiin tulee olla helposti saatavilla ja toimenpiteet selkeästi määritelty. Toimintaohjeeseen tulee liittää valvovan viranomaisen yhteystiedot.

5.10 Seuranta

Kun kaikki tietosuoja-asetuksen velvoittamat toimenpiteet on suoritettu, eivätkä nämä vaadi enää suoria työtehtäviä siirrytään seurantavaiheeseen. Oleellisinta seurantavaiheessa on tietää miten poikkeustapauksissa tulee toimia ja miten sisäiseen dokumentaatioon pääsee käsiksi. Onnistunut tietosuoja-asetuksen noudattaminen vaatii myös läheistä yhteistyötä henkilötietojen käsittelijän kanssa.

Jos toimintatapoihin tai tietojärjestelmiin on tulossa oleellisia muutoksia, tulevat riskiarviot ja riskianalyysit tehdä uudelleen, ja on nämä dokumentoitava asianmukaisesti.

6 Yhteenveto

Yrityksen toiminnan aloittaminen on monivaiheinen tapahtumasarja jonka aikana yrittäjän tulisi tulla tietoiseksi, ja lähes asiantuntijaksi useasta erilaisesta säädöksestä, laista ja toimenpiteestä. Tämän voidaan kuvitella olevan yksi yrittäjäksi ryhtymisen kiehtovuutta, mutta tiedon hajanaisuus ja kontekstin puute voi joissain tapauksissa aiheuttaa enemmän päänvaivaa kun olisi varsinaisesti tarvetta.

Tämän työn tarkoituksena oli auttaa tässä tiedon hajanaisuudessa selventämällä asiakasyritykselle tietosuoja-asetuksen tärkeimpiä asioita teorian, esimerkein sekä muistilistan avulla. Oletuksena on, että työ auttaa osaltaan asiakasyritystä vastuiden määrittelyissä, omasta roolista sekä yhteistyössä henkilötietojen käsittelijän suuntaan. Tietomäärä kerättiin useasta eri lähteestä ja sisältövaliditeetin varmistamiseksi kootun aineiston käsitteet on yritetty määritellä mahdollisimman selkeästi.

Aineistotutkimuksen perusteella voidaan todeta onnistuneen osoitusvelvollisuuden ja tietosuoja-asetuksen implementoinnin koostuvan useasta eri toimenpiteestä, eri velvollisuuksien tiedostamisesta ja rekisteröidyn oikeuksien tunnistamisesta. Tietoturva kokonaisuudessaan koostuu useasta eri osa-alueesta, missä tietosuoja-asetus on vain yksi tekijä muiden joukossa, mutta varmistamalla henkilötietojen käsittelyn oikeudelliset perusteet, ja perehtymällä hiukan tietosuoja-asetuksen tärkeimpiin velvollisuuksiin, voidaan asiakassuhteet rakentaa heti alusta alkaen kestävälle pohjalle.

Tämä työ antoi tekijälleen katsauksen tietosuoja-asetuksen historiaan, laajempaan kontekstiin sekä sen käytännön toteutukseen. Työ aloitettiin tutustumalla aiheeseen liittyvään kirjallisuuteen ja tämän perusteella työlle rakennettiin teoriaosuus. Oppimista karttui melko laaja-alaisesti tietoturvan osalta, vaikka työn tavoitteiden mukaan siihen valittiinkin vain tietosuoja-asetukseen liittyvää informaatiota. Teoriaosuuden ja kertyneen tiedon perusteella yritykselle laadittiin muistilista tärkeimmistä asioista, joka auttaa tietosuoja-asetuksen ymmärtämisessä. Opinnäytetyö prosessina on ollut kokonaisuudessaan hyvin mielenkiintoinen ja opettavainen.

Lähteet

Painetut

Andreasson, A., Riikonen, J., Ylipartanen, A., Pajala, I. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Helsinki: Tietosanoma.

Hanninen, M., Laine, E., Rantala, K., Rusi, M., Varhela, M. 2017. Henkilötietojen käsittely - EU-tietosuoja-asetuksen vaatimukset. Helsinki: Kauppakamari.

Järvinen, P., Rousku, K. 2017. Työpaikan tietoturva opas. Tunnista uhat, hallitse riskit. Helsinki: Alma Talent.

Pyyhtiä, T. 2019. Digiajan johtajan käsikirja. Käytännönläheinen, helppolukuinen ja tiivis opas digiajan johtamiseen. Helsinki: BoD - Books on demand.

Salminen, M. 2009. Tietosuoja sähköisessä liiketoiminnassa. Helsinki: Kariston kirjapaino.

Toikko, T., Rantanen, T. 2009. Tutkimuksellinen kehittämistoiminta. Tampere: Tampereen Yliopistopaino.

Sähköiset

Brill, J. 2018. Mircrosoft's commitment to GDPR, Privacy and putting customers in control of their own data. Viitattu 1.5.2020. https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/

Elinkeinoelämän keskusliitto. 2020. Tietosuojavastaavan nimittäminen. Viitattu 18.5.2020. https://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/tietopaketti-yrityksille-on-aika-valmistautua-eun-yleiseen-tietosuoja-asetukseen/#5-2-7--Tietosuojavastaavan-nimitt-minen

Digiturvamalli. 2017. 6-käsittelyn oikeudenmukaisuus. Viitattu 18.5.2020. https://fakta.digiturvamalli.fi/gdpr-asetus/6-kasittelyn-lainmukaisuus

Eur-Lex. 2018. Document 31995L0046. Viitattu 1.5.2020. https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX%3A31995L0046

GDPR.EU. 2020. gdpr vs lgpd. Viitattu 1.5.2020. https://gdpr.eu/gdpr-vs-lgpd/

Khan, M. 2017. Companies face high cost to meet new EU data protection rules. Viitattu 1.5.2020. https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc

Kuchler, H. US small businesses drop EU customers over new data rule. Viitattu 1.5.2020. https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04

Tietosuojavaltuutetun toimisto. 2019a. Mikä on henkilötieto. Viitattu 1.5. 2020. https://tietosuoja.fi/mika-on-henkilotieto

Tietosuojavaltuutetun toimisto. 2019b. GDPR. Viitattu 1.5.2020. https://tietosuoja.fi/gdpr

Tietosuojavaltuutetun toimisto. 2019c. Seloste käsittelytoiminnasta. Viitattu 1.5.2020. https://tietosuoja.fi/seloste-kasittelytoimista

Tietosuojavaltuutetun toimisto. 2019d. Rekisterinpitäjän seloste käsittelytoiminnasta. Viitattu 1.5.2020. https://tietosuoja.fi/rekisterinpitajan-seloste-kasittelytoimista

Tietosuojavaltuutetun toimisto. 2019e. Henkilötietojen käsittelijän seloste käsittelytoiminnasta. Viitattu 1.5.2020. https://tietosuoja.fi/henkilotietojen-kasittelijan-seloste-kasittelytoimista

Tietosuojavaltuutetun toimisto. 2019f. Tietosuojavastaavan nimittäminen. Viitattu 1.5.2020. https://tietosuoja.fi/tietosuojavastaavan-nimittaminen

Tietosuojavaltuutetun toimisto. 2019g. Henkilötietojen käsittelijä. Viitattu 1.5.2020. https://tietosuoja.fi/henkilotietojen-kasittelijat

Tietosuojavaltuutetun toimisto. 2019h. Henkilötietojen käsittelijän velvollisuudet. Viitattu 1.5.2020. https://tietosuoja.fi/henkilotietojen-kasittelijan-velvollisuudet

Tietosuojavaltuutetun toimisto. 2019i. Arvioi riskit. Viitattu 1.5.2020. https://tietosuoja.fi/arvioi-riskit

Tietosuojavaltuutetun toimisto. 2019j. Vaikutusten arviointi. Viitattu 1.5.2020. https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto. 2019k. Osoitusvelvollisuus. Viitattu 1.5.2020. https://tietosuoja.fi/osoitusvelvollisuus

Tietosuojavaltuutetun toimisto. 2019l. Tietoturvaloukkaukset. Viitattu 1.5.2020. https://tietosuoja.fi/tietoturvaloukkaukset

Tietosuojavaltuutetun toimisto. 2019m. Tietosuojavastaavat. Viitattu 1.5. 2020. https://tietosuoja.fi/tietosuojavastaavat

Tietosuojavaltuutetun toimisto. 2019n. Rekisteröidyn oikeudet. Viitattu 1.5. 2020. https://tietosuoja.fi/rekisteroidyn-oikeudet

Tilastokeskus. 2019. Väestön tieto- ja viestintätekniikan käyttö. Viitattu 1.5.2020. http://www.stat.fi/til/sutivi/2019/sutivi_2019_2019-11-07_tie_001_fi.html

Kuviot

Liitteet

Liite 1: Verkkokaupalle toimitettu tiivistetty muistilista

Muistilista tietosuoja-asetuksen velvoittamiin tärkeimpiin toimenpiteisiin

Henkilötietojen käsittelyn tarve ja laajuus

01

Tärkeää
-Mitä henkilötietoja käsitellään
-Missä/Miten/Kuinka kauan henkilötietoja säilytetään
-Vain tarpeellisen tiedon keräys, käsittelylle perusteltavuus
-Luovutetaanko tietoja kolmansille osapuolille tai organisaation ulkopuolelle

Yhteistyö henkilötietojen käsittelijän kanssa

02

Tärkeää
-Sopimukset ja vastuun määrittelyt yhdessä henkilötietojen käsittelijän kanssa

Vastuuhenkilö tai tietosuojavastaavan nimittäminen

03

Tärkeää
-Vastuuhenkilön tai tietosuojavastaavan valinta

Seloste käsittelytoiminnasta

04

Tärkeää
-Seloste sisäiseksi dokumentaatioksi
-Tietosuojavaltuutetun toimiston mallipohja rekisterinpitäjälle:
https://tietosuoja.fi/documents/6927448/8323207/Mallipohja+rekisterinpit%C3%A4j%C3%A4lle+seloste+k%C3%A4sittelytoimista/bf9167e3-3f89-4a40-a284-9f438f3b6476

Tietosuojaseloste / rekisteriseloste

05

Tärkeää
-Tietosuojaseloste rekisteröidyn tiedottamiseksi henkilötietojen käsittelystä

Riskiarvio ja riskianalyysi

06

Tärkeää
-Riskiarviot, riskianalyysit ja toimenpiteet vastaamaan riskitasoa

Varautuminen tietoturvaloukkauksiin

07

Tärkeää
-Toimenpiteet tietoturvaloukkauksien varalle
-Tietosuojavaltuutetun toimistojen esimerkkejä tietoturvaloukkauksista ja milloin tulee ilmoittaa valvontaviranomaisille:
https://tietosuoja.fi/documents/6927448/8214536/Esimerkkej%C3%A4+tietoturvaloukkauksista/754c16aa-152e-4f15-a458-d1579c5ea4b2/Esimerkkej%C3%A4+tietoturvaloukkauksista.pdf

Dokumentointi, osoitusvelvollisuus ja läpinäkyvyys

08

Tärkeää
-Dokumentoi kaikki asiakirjat, sopimukset ja toimintaselosteet. Pidä ne helposti saatavilla

Seuranta

09

Tärkeää
-Seuraa toimintaympäristössä tapahtuvia muutoksia. Suorita riskianalyysit tarvittaessa muuttuvilla tiedoilla